L'ARRETE DU 15 JUIN 2012 RELATIF A LA SIGNATURE ELECTRONIQUE DANS LES MARCHES PUBLICS - MODE D'EMPLOI

La publication au journal officiel du 3 juillet 2012 de l'arrêté du 15 juin 2012 relatif à la signature électronique dans les marchés publics, qui abroge et remplace l'arrêté du 28 août 2006, marque une nouvelle étape de la dématérialisation des procédures. L'usage des certificats de signature dans les marchés publics n'est plus limité à une liste de catégories de certificats : tout certificat de signature conforme au référentiel général de sécurité, ou à des conditions de sécurité équivalentes, est désormais accepté dans les marchés publics. Les opérations de vérification de la signature électronique sont précisées, et facilitées pour les certificats de signature figurant sur une liste de confiance. Les formats de signature à utiliser le plus couramment sont mentionnés. Visant l'automatisation la plus intégrée possible de l'usage de la signature électronique et de ses contrôles, ce texte permet le développement d'un outil indispensable à la dématérialisation des procédures.

Le guide pratique de la dématérialisation des marchés publics est en cours de révision pour tenir compte de cet arrêté.

1. Un impératif : la mise en conformité des profils d'acheteurs par rapport au référentiel général de sécurité (RGS) au plus tard le 19 mai 2013

Qu'ils soient considérés comme des systèmes d'information à part entière, ou une partie seulement de ceux-ci, les profils d'acheteurs, doivent, au plus tard le 19 mai 2013, être configurés pour utiliser les produits de signature électronique conformes au référentiel général de sécurité, tel qu'approuvé par arrêté du 6 mai 2010 (tous les documents sont accessibles sur le portail de la direction générale de la modernisation de l'Etat à l'adresse suivante : *www.references.modernisation.gouv.fr*).

Cette obligation n'est pas propre aux marchés publics, puisqu'elle s'applique à tous les systèmes d'information entrant dans le champ de l'ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives, et entre les autorités administratives (voir notamment son article 14.)

2. Un objectif : banaliser l'usage de la signature électronique dans les marchés publics en toute sécurité

2.1. A qui s'adresse ce texte? (article 1er de l'arrêté)

A tous les utilisateurs potentiels des marchés publics : autorités administratives et opérateurs économiques.

2.2. Quels sont les documents concernés ? (article 1er de l'arrêté)

L'arrêté ne crée pas de nouvelle obligation en matière de signature : tous les documents papiers signés de manière manuscrite ont la même valeur que les documents dématérialisés signés électroniquement. La signature du document peut être requise soit par les textes (le code des marchés publics impose la signature de l'acte d'engagement dans les procédures formalisées), soit dans les documents de la consultation ou dans les documents contractuels.

2.3. Est-il possible de limiter les certificats de signature électronique acceptés ? (article 2-I de l'arrêté) De limiter les formats de signature ? (article 3 de l'arrêté) Peut-on imposer l'utilisation de l'outil de signature proposé sur le profil d'acheteur ?

Dès lors que les certificats de signature utilisés sont conformes au RGS, ou garantissent un niveau équivalent de sécurité, l'acheteur ne peut les refuser. Par conséquent, les profils d'acheteurs doivent être en mesure, au moins, de traiter et d'accepter tous les certificats de signature conformes au RGS.

L'opérateur économique est donc libre d'utiliser le certificat de son choix si celui-ci remplit les obligations minimales équivalentes à celles du RGS. Il s'assure que le certificat qu'il utilise est au moins conforme au niveau de sécurité préconisé sur le profil d'acheteur, et donne tous les éléments nécessaires à la vérification de cette conformité au RGS par le profil d'acheteur.

Par ailleurs, une décision de la Commission européenne de février 2011 impose d'accepter les formats de signature XAdES, PAdES et CAdES cités à l'article 3 de l'arrêté. Les trois formats doivent être acceptés par le profil d'acheteur, qui peut néanmoins prévoir d'accepter des formats supplémentaires. Cette possibilité est alors mentionnée dans les documents de la consultation ou la lettre de consultation.

Tout outil de signature conforme à ce qui précède est utilisable. L'acheteur ne peut pas imposer l'emploi de l'outil de la plateforme. Néanmoins, lorsque l'opérateur économique utilise un autre outil de signature, il en permet la vérification en transmettant en parallèle les éléments nécessaires pour procéder à la vérification de la validité de la signature et de l'intégrité du document, et ce, gratuitement.

2.4. Comment vérifier la conformité du certificat de signature au RGS ? (article 2-II de l'arrêté)

L'ordonnance n° 2005-1516 du 8 décembre 2005 prévoit que l'autorité administrative détermine pour chaque système d'information, et après étude, le niveau de sécurité requis parmi les niveaux prévus par le RGS (niveau *, ** ou ***). Les échanges intervenant via le système d'information doivent par la suite respecter les règles correspondantes. Par exemple, si le profil d'acheteur requiert un niveau de sécurité ** du RGS, tous les produits utilisés sur le profil d'acheteur, dont le certificat de signature électronique, devront correspondre au moins aux préconisations du niveau ** du RGS. Cela signifie que la plateforme devra reconnaître et accepter les produits de niveau ** et ***, mais pas ceux de niveau *.

L''arrêté prévoit plusieurs cas selon le certificat de signature utilisé :

- ***le certificat de signature émane de la liste de confiance française ou d'une liste de confiance d'un autre Etat-membre (pour les certificats qualifiés, équivalents au niveau 3* du RGS),*** c'est-à-dire qu'il peut être relié à un prestataire ou un produit de sécurité référencé pour la France par le ministère chargé de la réforme de l'Etat sur le site *www.references.modernisation.gouv.fr;* et pour les autres Etats-membres par la Commission européenne sur le site *(http://ec.europa.eu/information_society/policy/esignature/eu_legislation/trusted_lists/index_en.htm).*

  Dans ce cas, la conformité du produit au RGS est présumée, et les seules vérifications à opérer sont celles du niveau de sécurité (*, ** ou ***) et bien sûr, de la validité de la signature elle-même. Le signataire n'a pas à fournir d'autres éléments que ceux permettant la vérification de la validité de la signature.

- ***le certificat de signature électronique n'est pas référencé sur une liste de confiance*** : il peut s'agir de produits émanant de prestataires de pays-tiers, mais aussi de prestataires européens ou français, qui n'ont pas fait l'objet d'un référencement, souvent pour des raisons de coût. Ce sont ces certificats qu'il faut vérifier avant de les accepter. L'arrêté prévoit que le signataire transmet les éléments nécessaires à cette vérification, en plus des éléments nécessaires à la vérification de la validité de la signature elle-même. Cela peut être l'adresse du site internet de référencement dans le pays tiers, une preuve de la qualification du prestataire ou du produit, l'adresse de l'autorité de certification qui a délivré le certificat de signature, qui mentionne la politique de certification…

2.5. L'acheteur est-il tenu d' effectuer lui-même ces vérifications techniques?

Non. La vérification des certificats de signature électronique et de la validité de la signature elle-même font partie actuellement des fonctionnalités d'un profil d'acheteur, sans que l'acheteur ait dû se doter des compétences techniques pour les examiner. L'automatisation et la traçabilité des vérifications et contrôles doivent continuer à être privilégiées. Le secteur s'y est préparé : le RGS est connu depuis mai 2010, et l'ordonnance du 8 décembre 2005 a prévu une mise en conformité progressive : seuls les systèmes d'information créés avant mai 2010 restent à mettre en conformité. Les autres sont en théorie conformes au RGS depuis, au plus tard, mai 2011.

En revanche, la vérification de l'identité du signataire, et de sa capacité à engager l'entreprise, reste, comme pour les marchés non dématérialisés, effectuée par l'acheteur.

Enfin l'examen automatique de la signature électronique n'exonère pas l'acheteur de sa responsabilité si la candidature ou l'offre est rejetée à tort pour des raisons techniques.

2.6. Que faire pendant la période de transition ?

L'arrêté est applicable dès le 1er octobre 2012, ce qui signifie qu'à cette date tous les certificats de signature doivent pouvoir être traités par les profils d'acheteurs pour examiner leur conformité avec le RGS, et vérifier la validité de la signature. En outre, les certificats dits « PRIS V1 » peuvent être encore utilisés jusqu'au 18 mai 2013, date à laquelle ils disparaîtront. La liste des catégories de certificats est disponible à l'adresse suivante : **http://www.entreprises.minefi.gouv.fr/certificats/**.

Les profils d'acheteurs doivent donc être en mesure de traiter automatiquement les deux types de certificats, et de lire et contrôler les formats de signature les plus courants.

Il est recommandé de préciser dans les documents de la consultation :

- un rappel du niveau de sécurité requis sur le profil d'acheteur (cf supra point 2.4. : niveau *, ** ou *** conforme au RGS) ;
- les documents pour lesquels une signature manuscrite ou le cas échéant électronique est requise ;
- Les formats de signature autorisés (et toujours au moins, les trois formats cités à l'article 3 de l'arrêté) ;
- Le rappel à titre pédagogique de certaines règles courantes : un zip signé ne vaut pas signature de chaque document du zip, une signature manuscrite scannée n'a pas d'autre valeur que celle d'une copie et ne peut pas remplacer la signature électronique…